NIH Application/System Security Plan (SSP) Template for Applications and General Support Systems

April 8, 2004

National Institutes of Health
Office of the Deputy Chief Information Officer
Information Security and Awareness Office
10401 Fernwood Rd.
Bethesda, Maryland 20817

Contents

Executive Summary

- The Executive Summary provides a quick management-level reference. It should be a one-page summation of the major aspects of the System Security Plan (SSP).
- The SSP is a managerial planning document required by the Computer Security Act and OMB Cir. A-130.
- The SSP should be consistent with the NIH Master Enterprise Security Plan and the companion NIH IT Security Requirements document. The SSP must also be consistent with the SSPs of any NIH General Support Systems (e.g., NIHnet, NIH Data Center) that the system depends on.
- Make sure every page of the SSP is prominently labeled "SENSITIVE" in the header, footer, or watermark.

A Application/System Identification

A.1 Application/System Category

- Indicate whether the application/system is an Application, Major Application (MA) or a General Support System (GSS):

  An Application is a term used to define a collection of information resources (hardware, software, people) used to satisfy a specific set of user requirements, but is not considered a GSS or an MA. Examples include programs on user desktops or a web or client/server application used by an office or IC.

  A Major Application (MA) is "an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." Within NIH, the MA classification includes, but is not limited to, such applications as the Administrative Database (ADB), Central Accounting System (CAS), and the NIH Business System (NBS).

  A General Support System (GSS) is an "interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people." Examples of General Support Systems at NIH include NIHnet, Parachute, the Data Centers, and most intranets.

- Due to the HHS & NIH IT consolidation program, NIHnet is defined as "extending to the wallplate" so that subordinate LAN/WANs need not create detailed SSPs, but need to document aspects which differentiate the LAN/WAN from NIHnet (such as those requiring greater or additional IT Security than what NIHnet calls for).

A.2 Application/System Name/Title

- Unique identifier & name given to the application/system

- Note that NIH Senior Management has determined that no NIH IT Application/System or Data shall be "Classified," so if you find otherwise in this regard, contact the NIH Chief Information Security Officer (CISO) in ODCIO.

A.3 Responsible Organization

- Organization responsible for the application/system

A.4 Information Contact(s)

- The owner(s) of the application/system and at least one other manager expertly knowledgeable about it.
  - Name
  - Title
  - Address
  - Phone Number
  - Fax Number
  - E-mail Address

A.5 Assignment of Security Responsibility

- Person(s) responsible for security of the application/system and an alternate emergency contact.
  - Name
  - Title
  - Address
  - Phone Number
  - Fax Number
  - E-mail Address

A.6 Application/System Operational Status

- If more than one status is selected, list which part(s) of the application/system are covered under each status designation.
  - Operational
  - Under Development
  - Undergoing a major modification

A.7 General Description/Purpose

- Describe the function or purpose of the application/system and the information processed.
- Describe the processing flow of the application/system from input to output.

- List user organizations (internal & external) and the type of data and processing provided.
- Describe roles and responsibilities of all users having access to the application/system. Include approximate number of authorized users and their physical location.

A.8 Application/System Environment

- Provide a general description of the technical application/system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.) Include a diagram of architecture here or in an appendix, if applicable.
- Describe the primary computing platform(s) used and a description of the principal application/system components, including hardware, software, and communications resources.
- Include any security software protecting the application/system and information.
- List the physical location(s) of the application/system.

A.9 Application/System Interconnection/Information Sharing

HHS & NIH policy requires that a memorandum of understanding (MOU) or memorandum of agreement (MOA) be obtained prior to connection with other applications/systems and/or sharing sensitive data/information. This section should list any such agreements. A sample NIH System Interconnection Security Agreement (ISA) is available at http://irm.cit.nih.gov/security/sec_policy.html. The written authorization should detail the rules of behavior and controls that must be maintained by the interconnecting systems.

- List names of any applications/systems interconnected to this entity.
- If connected to an external application/system that features lesser IT security controls than are used for this entity, or is not covered by an adequate security plan, provide a brief discussion of any security concerns that need to be considered for protection.
- A description of the rules for interconnecting applications/systems and for protecting shared data must be included with this security plan. See Sect. B.3, Rules of Behavior.

A.10 Applicable Laws or Regulations Affecting the Application/System

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the application/system.

A.11 Information Sensitivity and Criticality Assessment

The instructions for determining a Systems Criticality Level and Score are detailed in Sections 5.1 to 5.5 (pages 31 to 37) of the HHS Certification & Accreditation Guide. Because determination of the Certification Tier Scale and associated Level of Effort is very important for determining what will be required in the Certification and Accreditation (C&A) and SSP for this Application/System, those instructions should be followed in detail. This section provides only quick reference and may not be sufficient for the detailed process of computing the required Score and Tier Scale Level of Effort.

System Criticality:

System criticality is determined based on how integral the system is in carrying out the mission of the Institute it supports, NIH, and HHS. The criticality levels are as follows.

	Mission Critical (MC)	Automated information resources whose failure would preclude the HHS from accomplishing its core business operations.	3
	Mission Important	Automated information resources whose failure would not preclude the HHS from accomplishing core business processes in the short term (few hours), but would cause failure in the mid to long term (few hours to few weeks).	2
	Mission Supportive	Automated information resources whose failure would not preclude the HHS from accomplishing core business operations in the short to long term (few hours to few weeks), but would have an impact on the effectiveness or efficiency of day-to-day operations.	1

Criticality Score: 3/2/1

Data Sensitivity:
Data sensitivity is defined in terms of confidentiality, integrity, and availability. Each sensitivity criteria is rated on a scale as follows: High = 3, Medium = 2, and Low = 1. These scores are added together to calculate the Data Sensitivity Score. The sensitivity criteria are defined as follows.

- **Confidentiality** Assurance that information in an IT system is not disclosed to unauthorized persons, processes, or devices.
- **Integrity** Assurance that information in an IT system is protected form unauthorized, unanticipated, or unintentional modification or destruction.
- **Availability** Assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.

Confidentiality	H/M/L	3/2/1
Integrity	H/M/L	3/2/1
Availability	H/M/L	3/2/1

Sensitivity Score:
The Criticality and Sensitivity Scores are added together to determine the HHS Certification Score.

HHS Certification Score and Tier Levels:

	Tier Level	Certification Score

	Tier 0	4
	Tier 1	5-6
	Tier 2	7-8
	Tier 3	9-10
	Tier 4	11-12

Types of Sensitive Information:
Place a check (✓) next to the types of data found in the system. Provide any additional information about a particular type of information in the field to the right of the information type.

___ Patient Information
___ Privacy Act
Health/Physical
___ Condition
___ Financial
Investigatory or
___ Personnel
___ Time Critical
___ Diagnostic Information
___ Clinical Center Trials
___ Grants
___ Contracts
___ Research/Scientific Data
___ Other

A.12 Privacy Impact Assessment

State the date of the last Privacy Impact Assessment.

B Management Controls

This section describes the management control measures that are intended to meet the protection requirements of the National Institutes of Health (NIH) [system]. Management controls focus on the management of the IT security for a system and the management of risk for a system.

B.1 Risk Assessment and Management

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the application/system. Make sure the methodology specifically identifies threats, vulnerabilities, and additional security controls required/implemented to mitigate risks.
- List the group that conducted the assessment, and the date(s) the review was conducted.

- If there is no application/system risk assessment, include a milestone date (month and year) for completion of the assessment. If the risk assessment is more than 3 years old, or if a major modification has occurred since the previous risk assessment, make sure the SSP includes a milestone date for completion of a follow-up risk assessment.

B.2 Review of Security Controls

- List any independent security reviews conducted on the application/system in the last three years.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

B.3 Rules of Behavior

- A set of rules of behavior in writing must be established for each application/system that is Tier 2 or above. The rules of behavior should be made available to every user prior to the user receiving access to the application/system, with a signature page to acknowledge receipt. You can cite the NIH General IT Rules of Behavior at http://irm.cit.nih.gov/security/nihitrob.html, and just note any additional rules for your system.
- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the application/system. They should state the consequences of inconsistent behavior or non-compliance. They should also include appropriate limits on interconnections to other application/systems.
- Attach the rules of behavior for the application as an appendix and reference the appendix number in this section or insert the rules into this section.

B.4 Planning for Security in the Life Cycle

Although a computer security plan can be developed for an application/system at any point in the life cycle, the recommended approach is to design the plan at the beginning of the computer system life cycle. It is recognized that in some cases, at any one time the application/system may be in several phases of the life cycle. For example, a large human resources system may be in the operation/maintenance phase, while an older, batch-oriented input sub-system is being replaced by a new, distributed, interactive user interface. In this case, the life cycle phases for the application/system include the disposal phase (data and equipment) related to the retirement of the batch-oriented transaction system, the initiation and acquisition phase associated with the replacement interactive input system, and the operations/maintenance phase for the balance of the application/system.

In this section, determine which phase(s) of the life cycle the application/system, or parts of the application/system, are in. Identify how security has been handled during each of the listed applicable life cycle phases.

- Initiation
- Development/Acquisition
- Implementation

- Operation/Maintenance
- Disposal

If the system is in the development/acquisition phase, make sure the SSP contains the following information:

- security requirements that are identified during the design phase.
- security controls that test the procedures developed before procurement.
- solicitation documentation that includes security requirements and evaluation/test procedures.

If the system is in the implementation phase, make sure the SSP contains the following information:

- description of when design review and system tests were conducted and who conducted them.
- testing schedule and procedures for controls implemented after initial testing and acceptance.
- references to test procedure documentation.
- description of whether such documentation is kept up to date

If the system is in the operational phase, make sure the SSP contains the following information:

- description of the security operations and administration, including information pertaining to backup procedures, training for users and administrators, management of cryptographic keys, maintenance of user and administrative privileges, and updating security.
- description of the process for ensuring operation assurance.
- description of auditing processes used to maintain system operational assurance.

If the system is in the disposal phase, make sure the SSP contains the following information:

- requirements and procedures for secure transfer and/or long-term storage of data.
- requirements and procedures for media sanitization.

B.5 Certification and Accreditation

Certification consists of a technical evaluation of a sensitive application to see how well it meets security requirements. Accreditation is the official management authorization for the operation of an application and is based on the certification process as well as other management considerations. Accreditation is also referred to as authorization to process (ATP), which is the term most commonly used at NIH. Certification (or recertification) is required at least once every three years, as required by OMB Circular A-130, Appendix III. An application must also be recertified if the system undergoes a major modification. The source for HHS guidance on this subject is the HHS Certification & Accreditation Guide.

An accrediting official uses the certification report to evaluate certification evidence, decides on the acceptability of the security safeguards, approves corrective actions, ensures the corrective actions are implemented, and issues the accreditation statement. FIPS PUB 102 suggests that the accrediting official could be the application system manager, however the more sensitive the application, the higher the management level of the accrediting official should be.

[Describe who is responsible for certifying and accrediting the system, the process for performing the C&A, when those actions occurred, and what the results were. Cite any document supporting the certification and accreditation of the system. Also describe the C&A performed on any NIH enterprise systems or other NIH systems that apply to infrastructure or other components that support the system but are not covered by the system's C&A.]

- Provide the date of authorization, name, and title of management official authorizing processing in the application/system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request.
- Attach Certification and Accreditation memos, if they exists (see Appendices A and B).

C Operational Controls

This section describes the operational control measures that are intended to meet the protection requirements of National Institutes of Health (NIH) [system]. Operational controls are security controls that are primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise, and often rely upon management activities as well as technical controls.

C.1 Personnel Security

- Have all positions been reviewed for sensitivity level? (See http://irm.cit.nih.gov/security/table3.htm)
- Have individuals received background screenings appropriate for the position to which they are assigned?
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?
- Describe the process used for requesting, establishing, issuing, and closing user accounts.

C.2 Physical and Environmental Protection

- Discuss the physical protection in the area where application/system processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.). If the application/system resides in a data center, you can reference the SSP for the data center and note any differences.
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.
- Describe controls to prevent data interception from direct observation, interception of data transmission, and electromagnetic interception.

C.3 Production, Input/Output Controls

In this section, provide a synopsis of the procedures that support the operations of the application/system. Describe the controls used for the marking, processing, storage, and disposal of input and output information and media as well as the labeling and distribution procedures for information and media. The controls used to monitor the installation of application/system software updates should also be listed. Below is a sampling of topics that may be reported in this section.

- Are there procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
- Are there procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media?
- Are there audit trails for receipt of sensitive inputs/outputs?
- Are there procedures for restricting access to output products?
- Is there internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary?)
- Is there external labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)?
- Are there audit trails for inventory management?
- Is there a media storage vault or library containing physical, environmental protection controls/procedures?
- Are there procedures for sanitizing electronic media for reuse?
- Are there procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse?
- Are there procedures for shredding or other destructive measures for hardcopy media when no longer required?

State whether or not the application/system employs Configuration Management (controls and documents changes to the application/system and its operational environment, and assesses the IT Security impact of any changes), and in what manner it does. If it does not, state why and/or when it will be implemented.

C.4 Contingency Planning and Disaster Recovery

- Briefly describe the procedures (contingency plan) that would be followed to ensure the application/system continues to be processed if the supporting IT application/system were unavailable. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan may be attached as an appendix. Include descriptions for the following:
  - Agreements of backup processing
  - Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup)
  - Location of stored backups and generations of backups
- Are tested contingency/disaster recovery plans in place? How often are they tested? If a disaster recovery plan exists, reference it or attach it as an appendix.
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?
- Coverage of backup procedures, e.g., what is being backed up?

C.5 Application/System Configuration Management Controls

- Are there restrictions/controls on those who perform hardware and software maintenance and repair activities?
- Are there special procedures for performance of emergency repair and maintenance?
- Are there procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?
- Are there procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements?
- Are software warranties managed to minimize the cost of upgrades and cost-reimbursement or replacement for deficiencies?
- Was the application/system software developed in-house or under contract?
- Does the government own the software? Was it received from another agency?
- Is the application/system software a copyrighted commercial off-the-shelf product or shareware?
- Has the software been properly licensed, and have enough copies been purchased for the application/system?
- Are there organizational policies against illegal use of copyrighted software and shareware?
- Are periodic audits conducted of users' computers to ensure that only legal licensed copies of software are installed?
- What products and procedures are used to protect against illegal use of software?

- Describe any formal change control process in place.
    - Is there version control that allows association of application/system components to the appropriate application/system version?
    - Are all changes to the application/system software or application/system components documented?
    - Are there impact analyses to determine the effect of proposed changes on existing security control to include the required training for both technical and user communities associated with the change in hardware/software?
    - Are there change identification, approval, and documentation procedures?
    - Are there procedures for ensuring contingency plans and other associated documentation are updated to reflect application/system changes?
- Does the change control process require that all changes to the application/system software be tested and approved before being put into production?
- Are there procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production?
- Is test data live data or made-up data?
- Do test plans trace back to the original security requirements?
- Are test results documented?

C.6 Data Integrity/Validation Controls

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Are reconciliation routines used by the application/system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are integrity verification programs used by the application/system to look for evidence of data tampering, errors, and omissions?
- Is an intrusion detection tool installed to monitor the application/system?
- Are procedures in place to handle and close out security incidents?
- Are other network security software packages used?
- Is application/system performance monitoring used to analyze performance logs in real time to look for availability problems, including active attacks, and application/system and network slowdowns and crashes?
- Is penetration testing performed on the application/system? If so, what procedures are in place to ensure that tests are conducted appropriately?
- Is message authentication used in the application/system to ensure that the sender of a message is known and that the message has not been altered during transmission?

- If the application/system is involved with "the remote authentication of individual people over a network, for the purpose of electronic government and commerce," then the E-Authentication requirements of OMB Memorandum M-04-04 and NIST Special Pub. 800-63 "Draft Recommendation for Electronic Authentication" need to be followed, including a declaration of which of the four levels of technical requirements and E-Authentication testing was performed, when it was performed, and with what results (See B.5 above & D.3 below).

C.7 Documentation

Documentation includes descriptions of the hardware and software, policies, procedures, and approvals related to automated information security in the application/system. Documentation should also include descriptions of user and operator procedures, and backup and contingency activities.

- List the documentation maintained for the application/system. Examples may include:
  - vendor documentation of hardware/software
  - functional requirements
  - design specifications
  - source code documents
  - testing procedures and results
  - records of verification reviews/site inspections
  - standard operating procedures
  - user rules/manuals
  - emergency procedures
  - contingency plans
  - risk assessments
- Describe the procedure used to update documentation.
- List the physical location of documentation.

C.8 Security Awareness and Training

- Describe the type and frequency of application/system-specific training provided to employees and contractor personnel (workshops, formal classroom, focus groups, role-based training, and on-the job training).
- Describe the procedures for assuring that employees and contractor personnel have been provided adequate training.
- Describe the awareness program for the application/system.

C.9 Incident Response Capability

- Are there procedures for reporting incidents handled either by application/system personnel or externally?
- Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories, e.g., vendor patches, exploited vulnerabilities?
- What preventative measures are in place, i.e., intrusion detection tools, automated audit logs, penetration testing?

D Technical Controls

This section describes the technical control measures that are intended to meet the protection requirements of the system. Technical controls are security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations, and should be consistent with the management of security within the [system owner].

D.1 Identification and Authentication

- Describe the application/system's user authentication control mechanisms (password, token, and biometrics).
- Indicate the frequency of password changes, describe how changes are enforced, and identify who changes the passwords (the user, the system administrator, or the application/system).
- Provide the following if an additional password system is used in the application/system:
  - password length (minimum, maximum)
  - allowable character set
  - password aging time frames and enforcement approach
  - number of generations of expired passwords disallowed for use
  - procedures for password changes (after expiration and forgotten/lost)
  - procedures for handling password compromise
  - procedures for training users and the materials covered
- Describe the level of enforcement of the access control mechanism (network, operating system, and application/system).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords associated with a user ID that is assigned to a single person).

- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords encrypted while in transmission, automatically generated, or checked against a dictionary of disallowed passwords).
- State the number of invalid access attempts that may occur for a given user ID or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all application/system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch application/systems).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifiers, and group user identifiers) and any compensating controls.
- Describe any use of digital or electronic signatures and the standards used. Discuss the management procedures for key generation, distribution, storage, and disposal. If digital signatures are used, the technology must conform with FIPS 186, Digital Signature Standard and FIPS 180-1, Secure Hash Standard issued by NIST, unless a waiver has been granted.
- If the application/system is involved with "the remote authentication of individual people over a network, for the purpose of electronic government and commerce," then the E-Authentication requirements of OMB Memorandum M-04-04 and NIST Special Pub. 800-63 "Draft Recommendation for Electronic Authentication" need to be followed, including a declaration of which of the four levels of technical requirements and E-Authentication testing was performed, when it was performed, and with what results (see C.6 & D.3).
- Make sure the following controls are stated. Describe:

  procedures for training users and the subjects that are covered.

  how biometric controls are used and implemented.

  how token controls are used and implemented

  cryptographic key management procedures for key generation, distribution, storage, entry, use, destruction, and archiving.

D.2 Logical Access Controls

- Discuss the controls in place to authorize or restrict the activities of users and personnel within the application/system. Describe hardware or software features that are designed to permit only authorized access to or within the application/system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists [ACLs]).
  - How are access rights granted? Are privileges granted based on job function?
  - Describe the application/system's capability to establish an ACL or register.

- Describe how users are restricted from accessing the operating system or other application/system resources not required in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the application/system outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the application/system automatically blanks associated display screens and/or disconnects inactive users. After what period of user inactivity does the application/system require the user to enter a unique password before reconnecting?
- Indicate if encryption is used to prevent access to sensitive files as part of the application/system access control procedures.
- Describe the rationale for electing to use or not use warning banners, and provide an example if banners are used.
- Make sure the following controls are stated. Describe:
    1. How separation of duties is enforced to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion.
    2. How the Access Control Lists (ACLs) are maintained.
    3. How often ACLs are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.
    4. Policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users.
    5. What other hardware or technical control is used to provide protection against unauthorized system penetration against unauthorized system penetration and other known Internet threats and vulnerabilities if the system is connected to the Internet or other wide area network(s).
    6. Any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required.
    7. How host-based authentication is used.

D.3 Public Access Controls

- If the general public accesses the application/system, discuss the additional security controls used to protect the application/system's integrity (This section may not apply for some GSS's). What additional controls are used to protect the confidence of the public in the application/system? Such controls include segregating information made directly accessible to the public from official agency records. Others may include:
    - Some form of identification and authentication
    - Access controls to limit what the user can read, write, modify, or delete

- Controls to prevent public users from modifying information in the application/system
- Digital signatures
- CD-ROM for on-line storage of information for distribution
- Copies of information for public access available on a separate application/system
- Controls to prohibit the public from accessing live databases
- Verification that programs and information distributed to the public are virus-free
- Audit trails and user confidentiality
- Application/system and data availability
- Legal considerations
- If the application/system is involved with "the remote authentication of individual people over a network, for the purpose of electronic government and commerce," then the E-Authentication requirements of OMB Memorandum M-04-04 and NIST Special Pub. 800-63 "Draft Recommendation for Electronic Authentication" need to be followed, including a declaration of which of the four levels of technical requirements and E-Authentication testing was performed, when it was performed, and with what results (See B.5 & C.6 above).
- Make sure I&A controls are stated as being used if applicable.

D.4 Audit Trails

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection and remediation? Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them (e.g., type of event, when the event occurred, user ID associated with the event, program or command used to initiate the event)?
- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if it records personal user information?
- Describe how frequently audit trails are reviewed and whether guidelines exist.
- Does the appropriate application/system level administrator review audit trails following a known application/system software problem, an unexplained application/system or user problem, or a known violation of existing requirements by a user?
- Make sure the following controls are stated. Describe:

  How audit trails are designed and implemented to record appropriate information to assist in intrusion detection.

  How audit trails are used as online tools to help identify problems other than intrusions as they occur.

How implemented audit trails are sufficient to establish what events occurred and who (or what) caused them.

How separation of duties between security personnel who administer the access control function and those who administer the audit trail is used and enforced.

How the appropriate system-level or application-level administrator reviews the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

How audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, are used in a real-time or near-real-time fashion.

E Appendix A - Sample Certification Memorandum

Security Certification Memorandum

To: Designated Approving Authority
Date:
From: Certification Official
Subject: Security Certification of [INFORMATION SYSTEM]

A security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the HHS and NIH policy on security accreditation. The attached security certification package contains the following items: (i) the current security plan for the information system; (ii) the security test and evaluation report; and (iii) the plan of action and milestones. The security controls listed in the security plan for the information system have been evaluated by [CERTIFICATION AGENT] using the verification techniques and the procedures described in the security test and evaluation report to determine if those controls are effective in their application.

Based on the results of the security test and evaluation activities, the actual vulnerabilities in the information system have been identified and a list of recommended corrective actions prepared. The plan of action and milestones describes the corrective measures that have been implemented or planned to reduce or eliminate the stated vulnerabilities in the information system.

Signature:
Title:
Enclosures:

F Appendix B - NIH Sample Accreditation Memo

[INFORMATION SYSTEM] CERTIFICATION MEMORANDUM

To: Information System Owner
From: Authorizing Official
Date:
Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

A security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the HHS and NIH policy on security accreditation. After reviewing the results of the security certification and the supporting evidence provided in the associated security certification package (including the current security plan for the information system, the security test and evaluation report, and the plan of action and milestones), I have determined that the confirmed vulnerabilities in the information system result in a residual risk to the operations/assets of this agency that is fully acceptable. Accordingly, I am issuing a full authorization to operate the information system in its existing operating environment; the system is accredited without any significant restrictions or limitations. [If there are restrictions, list them here.] This security accreditation is my formal declaration that appropriate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security accreditation of the information system will remain in effect as long as: (i) the required Plan of Action and Milestones reports for the system are submitted to this office in accordance with HHS and NIH policy; (ii) the confirmed vulnerabilities reported during the continuous monitoring process do not result in additional risk to the agency's operations/assets which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security authorizations (in accordance with federal or agency policy).

The information system owner should retain a copy of this letter with all supporting security certification and accreditation documentation as a permanent record.

Signature of Designated Approving Authority:
Title:

Enclosures:

G Appendix C – SSP Appendixes

The following are possible appendixes to a SSP. All are not required for every system. Refer to Table 8 of the HHS Certification and Accreditation Guide for a list of which documents are required for systems of a specific Tier Level.

a. Acronyms
b. Definitions
c. References - list (with links) of the applicable NIST publications, Federal Laws and Regulations, and HHS regulations
d. Rules of Behavior
e. System Interconnection Agreements (if applicable)
f. Memorandums of Understanding (if applicable)
g. Configuration Management Plan
h. Privacy Impact Assessment
i. Contingency Plan
j. Disaster Recovery Plan
k. Certification and Accreditation memos
l. Document History